Challenges in Security for Cyber-Physical Systems

Parthajit Mohapatra

ECE Department, Indian Institute of Science, Bangalore

3[rd] January 2015

Outline

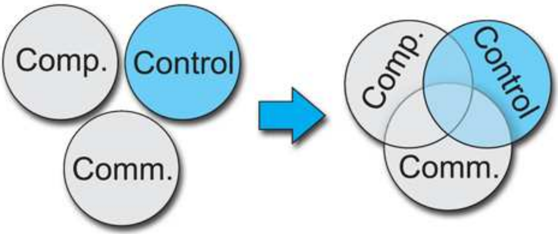
- Introduction to cyber-physical systems (CPS)
- Security issues
- Secure estimation
- Way forward

Atma-nirIkSaNa

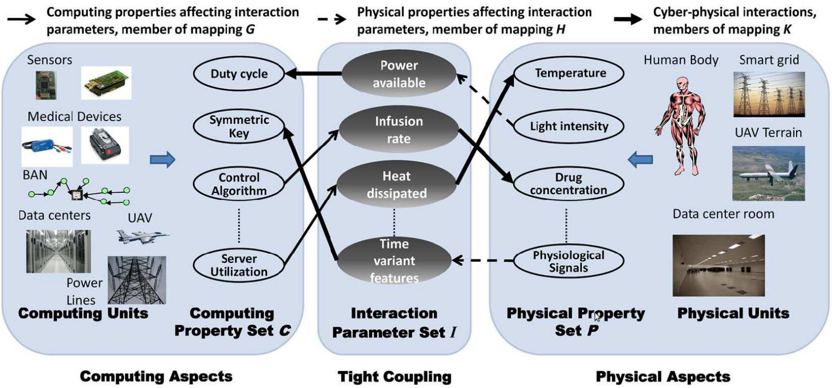
- Approximate capacity characterization
  - Low/moderate SNR
  - Limited CSI
- Precoder design algorithms
  - Asynchronism in communications
  - Acquiring CSI
- Information theoretic secrecy
  - Secure channel codes
  - Key-generation (at the physical layer)

Cyber-physical systems (CPS)

- New generation of systems that integrate computing and communication capabilities with the dynamics of physical and engineered systems



Cyber-physical systems (CPS)

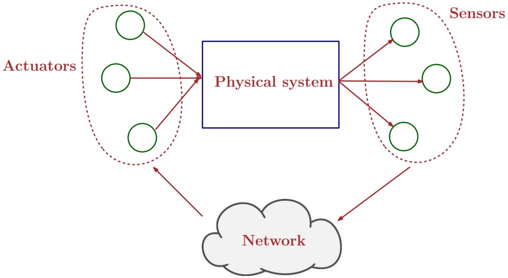


Examples of attacks on CPS

- Story of *Stuxnet* (2010)
  - Sophisticated computer worm that has spread through Iran, Indonesia and India, possibly build to destroy Iran's Bushehr nuclear reactor
  - Main target: programmable logic controller (PLC)
- Attack on sewage control system, Queensland (2000)
  - Attacker managed to hack into some controllers that activate and deactivate valves
  - Several months to figure out malfunctioning is due to attack
- There are many more examples of such attacks[1]

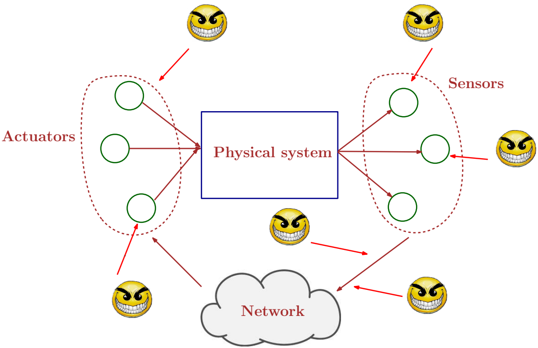
[1] A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in Proc. 3rd Conf. Hot Topics Security, 2008

Security for control system



- Control systems are becoming larger, distributed and open to the cyber world: vulnerable to attacks

Security for control system



- Will existing technique work?

No!

- Cryptography
  - Not suitable for active attacks
  - Distribution of keys and management
- Fault tolerant control system
  - Fixed number of failure modes
- Robust control
  - Bounded disturbances or known statistical model

Goal and major issues

Goal

Design secure control systems which is stable under attacks

Major issues

- Understand the consequences of an attack
- Attack-detection
- Attack-resilient strategies and architectures

Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks

Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi

IEEE trans. automatic control, June 2014

Setup

- Physical process modeled as a linear dynamical system

$$\mathbf{x}(t+1) = A\mathbf{x}(t) + B\mathbf{u}(t)$$

  $\mathbf{x}(t)$: state of the system at time t
  $\mathbf{u}(t)$: control input signal at time t

- p sensors monitor state of the plant ($\mathbf{y}(t) \in \mathcal{R}^p$)

$$\mathbf{y}(t) = C\mathbf{x}(t)$$

- Suppose there is attack on sensors[2]

[2]There can be attack on actuators also

Setup

- Linear dynamical system under attack

$$\mathbf{x}(t+1) = A\mathbf{x}(t) + B\mathbf{u}(t)$$
$$\mathbf{y}(t) = C\mathbf{x}(t) + \underbrace{\mathbf{e}(t)}_{\text{attack vector}}$$

- Some sensors are attacked
  - $\mathbf{e}_i(t) \neq 0$: attack on the i^{th} sensor
  - If sensor i is attacked, $\mathbf{e}_i(t)$ can be arbitrary

Setup

- Matrices A, B and C are known to the controller, but not $\mathbf{x}(0)$
- Controller choses action based on past observations
- Set of attacked sensors: $K \subset \{1, 2, \ldots, p\}$ and $q = |K|$
- K is fixed
- Attack can be on the sensors/communications links

Estimation problem

- Estimating the state of a linear dynamical system in the presence of attacks

$$\mathbf{x}(t+1) = A\mathbf{x}(t)$$
$$\mathbf{y}(t) = C\mathbf{x}(t) + \mathbf{e}(t)$$

- Control input can be discarded

Decoder

A decoder $D : (\mathcal{R}^p)^T \to \mathcal{R}^n$ corrects if it is resilient against any attack of q sensors[a]

$$D(\mathbf{y}(0), \ldots, \mathbf{y}(T-1)) = \mathbf{x}(0)$$

[a] At any instant of time q sensors are attacked

Correction of q errors

Proposition

Let $T > 0$ be fixed. Then q errors are correctable after T steps for the pair (A, C) if

$$\forall \mathbf{x} \neq 0 \qquad |\text{Supp}(C\mathbf{x}) \cup \text{Supp}(CA\mathbf{x}) \ldots \text{Supp}(CA^{T-1}\mathbf{x})| > 2q$$

- Dynamics should give redundancy
- e.g.: Good pairs

$$A = [0\,1\,0; 0\,0\,1; 1\,0\,0] \quad \text{and} \quad C = I$$

Some observations

- Condition

$$\forall \mathbf{x} \neq 0 \qquad |\text{Supp}(C\mathbf{x}) \cup \text{Supp}(CA\mathbf{x}) \ldots \text{Supp}(CA^{T-1}\mathbf{x})| > 2q$$

- Not easy to check
- Number of correctable errors does not increase beyond $T = n$ steps
- No more than $p/2$ errors can be corrected

Proposition

For almost all pairs (A, C), the number of correctable errors is maximal and equal to $\lceil \frac{p}{2} - 1 \rceil$

Optimal decoder

$$\text{minimize}_{\mathbf{x} \in \mathcal{R}^n, K \subset \{1,\ldots,p\}} |K|$$

subject to

$$\text{supp}(\mathbf{y}(t) - CA^t\mathbf{x}) \subset K, \text{ for } t \in \{0, 1, \ldots, T-1\}$$

- Decoder looks for the smallest set of attacked sensors that can explain the received data

Proposition

If q errors are correctable for a pair (A, C), then they can be corrected by the above decoder.

- Optimal decoder
- NP-hard

Results in CS come to rescue

- Relax the optimal decoder to make it computationally tractable
- ℓ_0 norm is replaced by $\ell_1|\ell_r$

$$[\mathbf{y}(0)| \quad \ldots|\mathbf{y}(T-1)] = [C\mathbf{x}| \quad \ldots|CA^{T-1}\mathbf{x}] + [\mathbf{e}(0)| \quad \ldots|\mathbf{e}(T-1)]$$

- Optimal decoder

$$D_0(\mathbf{y}(0),\ldots,\mathbf{y}(T-1)) = \arg\min_{\mathbf{x}\in\mathcal{R}^n} \quad ||Y(T)-\phi(T)\mathbf{x}||_{\ell_0}$$

- Magnitude of the row is measured by ℓ_r norm

$$D_{1,r}(\mathbf{y}(0),\ldots,\mathbf{y}(T-1)) = \arg\min_{\mathbf{x}\in\mathcal{R}^n} \quad ||Y(T)-\phi(T)\mathbf{x}||_{\ell_1|\ell_r}$$

where $||M||_{\ell_1|\ell_r} = \sum_{i=1}^{p} ||M_i||_{\ell_r}$

Relaxed decoder

Proposition

The following are equivalent

- Decoder $D_{1,r}$ can correct q errors after T steps
- For all $K \subset \{1, \ldots, p\}$ with $|K| = q$ and for all $\mathbf{x} \in \{R\} - \{0\}$, it holds

$$\sum_{i \in K} ||(\phi^T \mathbf{x})_i||_{\ell_r} < \sum_{i \in K^c} ||(\phi^T \mathbf{x})_i||_{\ell_r}$$

- Above condition guarantees that the row components of $\phi^T \mathbf{x}$ are sufficiently spread

Challenges

- Set of attacked sensors is varying
- When noise is present in the system

$$\mathbf{x}(t+1) = A\mathbf{x}(t) + B(\mathbf{u}(t) + \underbrace{\mathbf{a}(t)}_{\text{attack on actuators}}) + \underbrace{\mathbf{w}(t)}_{\text{noise}}$$

$$\mathbf{y}(t) = C\mathbf{x}(t) + \mathbf{e}(t)$$

- CS are in general non-linear
- Do not have proper knowledge of A and C

Other aspects/approaches

- Detection of attacks
  - Hypothesis testing
  - Consensus
- Secure distributed estimation
- Key management
- Secure routing
- Game theory analysis